Privacy e GDPR negli studi professionali (e legali) – Parte 2 – DPO e valutazione d'impatto

Come si applica in concreto il GDPR negli studi professionali, fra cui gli studi legali?
Parte 2: Quando nominare un DPO? Quando effettuare la valutazione d'impatto sulla protezione dei dati?

In questo precedente articolo: https://www.storaristudiolegale.it/blog/privacy-e-gdpr-negli-studi-professionali-e-legali-parte-1-ruoli-principali sono state individuate le prime tre figure chiave del trattamento dei dati personali (titolare del trattamento, responsabile del trattamento e soggetto autorizzato/incaricato).

Ulteriore figura fondamentale è quella del "***responsabile della protezione dei dati***" o "*Data Protection Officer*" (D.P.O.)

La **nomina** del D.P.O. da parte del titolare o del responsabile del trattamento è **obbligatoria nei casi** in cui: ***(a)*** il trattamento venga effettuato da un'autorità o un ente pubblico; ***(b)*** le attività principali del titolare o del responsabile del trattamento richiedano il monitoraggio regolare e sistematico degli interessati su larga scala; ***(c)*** le attività principali del titolare o del responsabile del trattamento consistano nel trattamento su larga scala di categorie specifiche di dati, ossia quelli di cui all'articolo 9 GDPR (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), nonché dati relativi a condanne penali e a reati (articolo 37, § 1, GDPR).

Il D.P.O. dev'essere designato in funzione delle sue **specifiche qualità professionali**, fra cui rientra il possesso di **conoscenze specialistiche** in materia di normativa e prassi sulla protezione dei dati, nonché la capacità di assolvere ai compiti – anche di natura tecnica – assegnati (articolo 37, § 5, GDPR). Tale figura può essere un dipendente del titolare o del responsabile del trattamento oppure un soggetto esterno con il quale viene stipulato un apposito contratto di servizi (articolo 37, § 6, GDPR).

Il D.P.O. dev'essere coinvolto in ogni questione riguardante la protezione dei dati personali (articolo 38 GDPR); fra i suoi compiti principali rientrano l'attività di **informazione e consulenza** rivolta al titolare e al responsabile del trattamento dei dati e l'attività di **sorveglianza** sul rispetto del GDPR, di altre disposizioni dell'Unione Europea o degli Stati membri, nonché delle politiche assunte dal titolare o dal responsabile del trattamento.

Il D.P.O. rappresenta anche il **punto di contatto** con il Garante per la protezione dei dati personali (articolo 39 GDPR), fermo restando che la responsabilità delle scelte sulle misure da adottare rimane

Verona - via Tonale, 16 - CAP 37126
T +39 045 8948362
F +39 045 9235363
studio@storaristudiolegale.it
–
storaristudiolegale.it

sempre ed esclusivamente in capo al titolare o al responsabile del trattamento per quanto di sua competenza.

Se richiesto, il D.P.O. fornisce un parere in merito alla "***valutazione d'impatto sulla protezione dei dati***" e ne sorveglia lo svolgimento secondo le prescrizioni dell'articolo 35 del GDPR.

*

La **valutazione d'impatto** (articolo 35 GDPR) **è un processo** di analisi e stima dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali, con particolare attenzione all'origine, alla natura, alla particolarità e alla gravità del rischio (considerando 84 GDPR).

L'oggetto della valutazione d'impatto è **la tipologia di trattamento** dei dati realizzata dal titolare, per suo conto o sotto la sua vigilanza, non il trattamento in sé.

Nella valutazione del rischio connesso al tipo di trattamento entrano in gioco la natura, l'ambito di applicazione, le finalità del trattamento, la giustificazione della necessità e della proporzionalità del trattamento rispetto alle finalità individuate, le fonti di rischio. **Esito** della valutazione è **l'individuazione delle misure di protezione**, quindi il complesso delle **garanzie** e delle **strategie** previste **per attenuare i rischi** identificati (considerando 90 GDPR).

La valutazione d'impatto, benché *in astratto facoltativa*, **può essere** *in concreto* ***necessaria*** **tutte le volte in cui è probabile che si presenti un rischio** (non qualsiasi ma) **elevato** per i diritti e le libertà delle persone fisiche, anche in considerazione dell'uso di nuove tecnologie, della natura, dell'oggetto, del contesto e della finalità del trattamento (articolo 35, § 1, GDPR; considerando 84, 89-93, 95 GDPR).

Il GDPR prevede espressamente i seguenti esempi di tipologie di trattamento che possono presentare rischi elevati: valutazione sistematica e globale di aspetti personali di persone fisiche, di profilazione di utenti; trattamento (su larga scala) di categorie particolari di dati personali; sorveglianza sistematica su larga scala di zona accessibile al pubblico (articolo 35, § 3, GDPR).

Altri criteri ulteriori sono stati forniti dal **WP29** (*Working Party article 29*, organismo così chiamato perché previsto dall'articolo 29 della direttiva 95/46/CE, oggi sostituito dall'*European Data Protection Board*), secondo il quale, **nella maggioranza dei casi, il titolare del trattamento può considerare che la valutazione d'impatto divenga necessaria in presenza di due (o, in alcuni casi, anche solo di uno) dei criteri stessi**, ossia: 1. trattamenti valutativi o di *scoring*, compresa la profilazione; 2. decisione automatizzata con effetto giuridico (es. stipula di assicurazione *online*); 3. monitoraggio

sistematico (es. videosorveglianza); 4. raccolta di dati sensibili, di natura giudiziaria o estremamente personali; 5. trattamento di dati personali su larga scala; 6. combinazione incrociata di dati che esula dal consenso iniziale (es. *Big Data*); 7. dati relativi a persone vulnerabili; 8. uso innovativo (es. riconoscimento facciale); 9. trattamenti che potrebbero impedire all'interessato di esercitare un diritto, avvalersi di un servizio o stipulare un contratto (es. *screening* dei clienti per la concessione di finanziamento).

*

Tenuto conto che il considerando 91 del GDPR precisa che "*Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato",* il **Consiglio Nazionale Forense** (Commissione Privacy, 22 maggio 2018) ha precisato che la **maggior parte degli studi legali**, non trattando dati personali "su larga scala", **non ha l'obbligo di nominare un D.P.O.**

Ciononostante, "*la valutazione dell'opportunità o meno di nominare un delegato alla protezione i dati deve essere effettuata caso per caso, in funzione in particolare dei seguenti parametri: - numero di persone interessate dal trattamento di dati personali; - volume dei dati trattati, - durata; - permanenza delle attività del trattamento; - estensione geografica dell'attività di trattamento*" (Consiglio Nazionale Forense – Commissione Privacy, 22 maggio 2018).

*

Quanto alla predisposizione della **valutazione d'impatto all'interno degli studi legali**, il Consiglio Nazionale Forense afferma che questa, "*per quanto non obbligatoria*", può rappresentare "***un'opportunità organizzativa*** *nell'ormai imprescindibile gestione dei trattamenti*" (Consiglio Nazionale Forense – Commissione Privacy, 22 maggio 2018).

È possibile che lo studio legale, oltre a raccogliere dati sensibili, di natura giudiziaria o estremamente personali (criterio n. 4 WP29), raccolga anche dati relativi a persone vulnerabili quali, ad esempio, minori, anziani, pazienti o vittime di reato (criterio n. 7 WP29).

Sul punto, il Consiglio Nazionale Forense afferma che "*la valutazione di impatto è* ***comunque necessaria*** *laddove vengano soddisfatti almeno due dei nove dei criteri indicati dal WP29"* (Commissione Privacy, 22 maggio 2018). In realtà, le linee guida del WP29 prevedono che "*un trattamento può corrispondere ai (nove, n.d.r.) casi di cui sopra ed essere comunque considerato dal titolare del trattamento un trattamento tale da non "presentare un rischio elevato". In tali casi il titolare*

del trattamento deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i punti di vista del responsabile della protezione dei dati".

*

Si declina qualsiasi responsabilità in merito alle informazioni qui rese, che i lettori sono onerati di verificare nell'interesse proprio e dei terzi con cui le condividono.

L'articolo è consultabile anche sul sito dello studio, sezione blog, al link:
https://www.storaristudiolegale.it/posts

Verona - via Tonale, 16 - CAP 37126
T +39 045 8948362
F +39 045 9235363
studio@storaristudiolegale.it
–
storaristudiolegale.it